Comments of the World Privacy Forum

To the Office for Civil Rights, Office of the Secretary, Department of Health and Human Services, regarding the NPRM proposing modifications to the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule), RIN Number 0945-AA20

Sent via www.regulations.gov

U.S. Department of Health and Human Services, Office for Civil Rights
Attn: HIPAA and Reproductive Health Care Privacy NPRM
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue SW
Washington, DC 20201

14 June 2023

The World Privacy Forum welcomes the opportunity to comment on the Department's Notice of Proposed Rulemaking (NPRM) amending the HIPAA Privacy Rule to modify the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). 88 Federal Register 23506 (April 17, 2023), https://www.federalregister.gov/d/2023-07517 .

The World Privacy Forum (WPF) is a nonprofit, non-partisan 501(c)(3) public interest research group.[1] WPF focuses on multiple aspects of privacy, with health privacy being among our key areas of work. We publish a large body of health privacy information, including guides to

[1] World Privacy Forum, https://www.worldprivacyforum.org/.

HIPAA; reports and FAQs for victims of medical identity theft; and materials on genetic privacy, precision medicine, electronic health records, and more.[2] We testify before Congress and federal agencies, and we regularly submit comments on HIPAA and related regulations. WPF participates in the World Health Organization as co-chair of the Research and Academia Network Constituency, and serves on its data governance workgroup. You can find out more about our work and see our reports, data visualizations, testimony, consumer guides, and comments at http://www.worldprivacyforum.org.

WPF supports the changes proposed in the NPRM. In the NPRM's overview, HHS states: "If individuals believe that their Protected Health Information (PHI) may be disclosed without their knowledge or consent to initiate criminal, civil, or administrative investigations or proceedings against them or others based primarily upon their receipt of lawful reproductive health care, they are likely to be less open, honest, or forthcoming about their symptoms and medical history." We agree with this statement regarding the chilling effects that medical mistrust can have on patients and their health outcomes, particularly for those in vulnerable communities that have been impacted by historic and ongoing health disparities.

We have a number of comments and suggestions to offer in response to the NPRM. We hope that our ideas will be helpful.

I. Section 1178(b) of the Social Security Act (42 U.S.C. § 1320d-7)

This provision of law protects public health reporting from HIPAA's normal preemption policy. The language protects and supports the "reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention."

The Department asks whether definitions for these terms are needed to make sure that reproductive health care information is not included as part of public health reporting. We believe that precision is essential here. Battles over aspects of reproductive health are being fought trench-by-trench and inch-by-inch. In our view, there are now and will be in the future those who may be willing to use every arguably legal method to collect information about those who seek, provide, or assist in lawfully provided reproductive health activities, including terminations of pregnancies.

We see no reason to assume that public health reporting will be overlooked in this fight. If the Department does not specify in express terms that reporting of reproductive health information is not permitted as part of public health reporting, surveillance, investigation, and intervention, then it is quite possible that one or more states will try to use the public health system as a tool in matters relating to lawful reproductive health matters, including lawful terminations of pregnancies. As long as there is a colorable argument that the statute and the rule do not expressly exclude regarding reproductive health information reporting, a battle over this issue might occur and continue for some years. We urge the Department to put itself and others in the best possible position to navigate this matter by adding express and unambiguous language to the rule.

---

[2] See World Privacy Forum, *A Patient's Guide to HIPAA,* https://www.worldprivacyforum.org/2019/03/hipaa/. See also our Health Category page for additional materials at https://www.worldprivacyforum.org/ category/health-privacy/.

In addition, we observe that any presumption about the scope of existing language in the law or in the rule could easily be reversed by another Administration. If the Department acts clearly now, it would take another rulemaking in order to overturn a position locked in place by a specific rule.

We have an additional observation. The discussion in the NPRM states:

> Thus, the Privacy Rule's exceptions for reporting of disease or injury, birth, or death do not allow the use or disclosure of PHI for investigating or punishing a person for seeking, obtaining, providing, or facilitating reproductive health care. Similarly, state laws requiring disclosure for such purposes are not exempt under section 1178(b) from HIPAA's general preemption provision.

We think that this statement is, unfortunately, somewhat misleading. There is a broader context that must be considered. Under well-established HIPAA principles, once a HIPAA covered entity discloses PHI to a third party who is not a HIPAA covered entity, the PHI is no longer covered by HIPAA in the hands of that third party. Nor does the Department currently have jurisdiction over or enforcement authority that can be used against a third-party recipient of PHI who is not a HIPAA covered entity. We know that the Department understands these points well.

The Department also understands that recipients such as public health authorities that receive PHI for a particular purpose are not, unless constrained by another statute, rule, attestation, or data use agreement, limited in how they use and disclose the PHI. We know of no general rule that would prevent PHI that passes through the hands of a public health authority from being provided to law enforcement authorities and used against anyone. Even if there were an exclusionary rule in a trial court, the exclusion of evidence at trial would not prevent a public health authority from disclosing information to a law enforcement agency for use in an independent investigation or prosecution.

In short, we think that the Department should nail closed every possible avenue that could lead to the collection, use, or disclosure of reproductive health care information for a law enforcement purpose. If that means expressly prohibiting disclosure of some reproductive health information or disclosure of other information potentially of interest to public health authorities that will not comply with limits, then so be it. We have a suggestion later in these comments for a way to bind public health authorities that goes beyond the Department's proposal for using attestations.

II. Public Health Surveillance, Investigation, or Intervention

The NPRM states:

> The Department also proposes to clarify that such public health activities do not include uses and disclosures for the criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing, or facilitating reproductive health care, or to identify any person for the purpose of initiating such an investigation or proceeding.

WPF agrees with the intent of this clarification. However, despite the good intent, it does not ensure that information lawfully disclosed for public health activities will never be used for criminal, civil, or administrative investigations or proceedings against any person. As discussed above, once a HIPAA covered entity discloses PHI to a third party who is not a HIPAA covered entity, the PHI is no longer covered by HIPAA in the hands of that third party. Nor does the Department have jurisdiction over or enforcement authority that can be used against a third-party recipient of PHI who is not a HIPAA covered entity.

The HIPAA privacy rule can limit when and why PHI may be disclosed by a HIPAA covered entity to a third party without consent, but it cannot control downstream uses and disclosures of that PHI by a third party who is not a HIPAA covered entity. We support the clarification of the definition of *public health*, but we do not see it as sufficient for the intended purpose.

We do not have a simple solution to the problem of controlling downstream activities by lawful recipients of PHI by those that are not HIPAA covered entities. One solution which we suggest in this regard is that the Department explore the possibility of mandating that public health disclosures be accomplished through a data use agreement (DUA).[3] This approach has some features that may be better than the attestation that the Department proposes. Specifically, a DUA can be as long and as detailed as necessary to prevent inappropriate uses and disclosures of PHI.

A DUA can impose limits (enforceable by the Department or, if allowed under the DUA, by data subjects or others) on the use and disclosure of information given to public health agencies pursuant to HIPAA. If every covered entity had to prepare and negotiate a DUA with every public health authority, we recognize that the task would be impossible. However, if the Department established the terms of a public health DUA and mandated that any public health agency receiving PHI from a HIPAA covered entity must abide by the terms of the agreement as a condition of receiving PHI, all of the work could be accomplished with a single nationwide DUA and a rule change. Some of the mechanics could be handled using the attestation method that the Department proposes later in this NRPM, but we think that a DUA may be better.

When a disclosure of PHI by a HIPAA covered entity includes reproductive health care information, a DUA could prohibit the recipient from using, reusing, or disclosing PHI to anyone seeking the PHI for any civil or criminal action against persons who seek, obtain, provide, or facilitate lawful reproductive health care. A DUA could establish additional rules to support the basic purpose. Importantly, a DUA could require a public health authority to impose on any downstream recipients the same terms as a condition of receiving the PHI.

It is not lost on us that the idea of requiring DUAs for downstream PHI recipients who are not HIPAA covered entities might have broader application. Some other privacy "loopholes" resulting from the application of HIPAA only to covered entities could be closed if other DUAs were required for other nonconsensual (and some consensual!) disclosures. We are not pursuing this idea more broadly here because the idea goes well beyond the scope of the current rulemaking. The

---

[3] We think that you may find useful ideas about DUAs in a law journal article by our colleague Robert Gellman. See *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 Fordham Intellectual Property, Media & Entertainment Law Journal 33 (2010), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1277&context=iplj. Take note of the article's discussion of third-party beneficiaries in DUAs.

Department might consider whether DUAs could play a bigger role in protecting against unwanted uses and disclosures of PHI provided to third parties, especially when the disclosures occur without the consent of the data subject.

III. Adding a Definition of "Reproductive Health Care"

We do not have any advice on the need for a definition of *reproductive health*. We are confused by the discussion about *reproductive health care* because it mentions the provision of medications and devices that include those that are available over-the-counter. We observe – and the Department well knows – that HIPAA only applies to covered entities. When HIPAA does apply, it applies to all PHI held by covered entities.

Those who sell over-the-counter medications are typically not covered entities (although some may be part of a hybrid entity). The sale of non-prescription prenatal vitamins by a merchant who is not a covered entity does not generate PHI subject to HIPAA. There may be a point here that we are not fully seeing, and in that case we offer our apologies. We nevertheless suggest that there may be a need for more clarity in this discussion with respect to activities conducted normally by those not subject to HIPAA.

IV. Clarifying When PHI May Be Used or Disclosed by Regulated Entities

The Department proposes to add an exception in § 164.502(a)(1)(iv) for uses and disclosures for investigations or proceedings associated with reproductive health care as prohibited by paragraph (a)(5)(iii). The Department seeks to preclude any possibility that a third party, such as a law enforcement official, could obtain an individual's PHI for a prohibited purpose by coercing the individual to sign an authorization. We support this change, and we applaud the Department for recognizing the potential loophole here. We can envision a law enforcement official offering a patient immunity if the patient signs an authorization that will share information about those who assisted with a reproductive health procedure and who may be the subject of investigation and prosecution.

Even though it is helpful, however, the proposed language does not fully solve the problem. We see two different types of problems.

First, a clever law enforcement official or entity could set up an apparently separate office for "Patient Health Care Assistance" and request that individuals consent to sharing PHI with that office. No one at a covered entity would necessarily recognize the connection between the patient assistance office and law enforcement. Law enforcement officials could also work with a wholly separate and possibly private, non-HIPAA covered organization that positions itself to counsel women regarding reproductive health choices. If women made choices that the counseling organization disagreed with, the entity could give patient records to law enforcement authorities or other parties, as the entity would be unconstrained by HIPAA. We remind the Department of the point we made earlier that once a non-HIPAA covered entity obtains PHI, that PHI can be used and disclosed without regard to the restrictions in HIPAA.

Second, in section § 164.524(c)(3)(ii) of the existing rule, a provision mandates that a covered entity must transmit a copy of an individual's PHI to another person designated by the individual. The language here is absolute. It does not allow a covered entity to question why the individual wants to share their PHI with a third party. If a data broker, marketer, criminal, or scammer obtains consent from an individual, the rule does not allow a covered entity any opportunity for intervention. The only allowable response is disclosure.

We objected to the breadth of this provision in comments on an earlier rulemaking. Wheedling consent from an individual is rarely a problem for anyone who has power over that individual, even if that power is only a minimal ability to deny access to a website, or giving a coupon for a discount. In short, scammers are likely to have little to no difficulty obtaining consent for sharing PHI with a third party. We know that as things stand now, scammers successfully receive thousands or hundreds of thousands of dollars from naïve and even some discerning individuals. Those who want to influence the reproductive health choices of patients could try to collect health information posing as reporters, researchers, pollsters, or others, and if this type of social engineering worked even one time, full health records could be turned over to non-covered entities, with potentially significant negative consequences. Relatively few patients know all of the HIPAA rules, and it is the rare individual who will understand in advance how HIPAA protections change after consent for sharing is given.

While we recognize that covered entities should not be able to block patient directions to share their PHI in many cases, we believe that covered entities should, at a minimum, have a limited ability to ask an individual about their choice to share PHI. The breadth of the Department's earlier decision to allow unrestricted sharing of PHI completely outside the protections of HIPAA now comes back to haunt the Department's attempt to restrict the disclosure of reproductive health information. Even in the face of likely coerced consents in matters involving reproductive health, the Department doubles down on its insistence that patient access is a higher priority than any other concern.

We see § 164.524(c)(3)(ii) in conflict with proposed § 164.502(a)(1)(iv). The NPRM discusses the possibility that a patient could be coerced into using the ability to direct transmission to another person, including a law enforcement official. While the Department recognizes the problem, it washes its hands by saying that the right of a patient to direct transmission of their record is "paramount." In other words, the proposal seeks to block one loophole that would allow law enforcement officials to obtain PHI with patient consent, but it does not block another equivalent loophole that can be used merely by citing a different provision of the rule.

Law enforcement officials wanting reproductive health information will immediately learn to use a consent form citing § 164.524 rather than a more standard authorization. The proposal to block coerced consents through an exception in § 164.502(a)(1)(iv) effectively could be meaningless.

We point out that once the rule allows or directs a covered entity to make an assessment of the purpose of an authorization (or other method) to allow a third party to obtain a copy of the individual's PHI, it is a small step to give covered entities broader authority. We recognize that there are circumstances in which a covered entity will want to deny a third-party access to PHI in

order to protect the covered entity's interests rather than a patient's interest. The Department can deal with that problem through more specific rules and through harsh penalties when it occurs.

We believe that, at a minimum, a covered entity should be able to question an individual's consent for disclosure § 164.524(c)(3)(II) to a data broker, marketer, or to an entity seeking to use the records for a fraudulent purpose.[4] The same should be true when anyone uses § 164.524(c)(3)(II) as a method for obtaining access to a patient's PHI. Even if a covered entity can only impose a procedural barrier by asking a patient the purpose of the authorization, that may be enough to prevent harmful sharing of PHI in many circumstances.

V. Attestations

The Department recognizes the problem that covered entities face when presented with requests for disclosure that call for the exercise of judgment. The NPRM's proposed solution is a requirement for attestations by those requesting PHI that the request is not for a prohibited purpose. This is a reasonable approach to the problem, but it is likely to have limited effectiveness.

We predict that many covered entities will respond to the provision by demanding an attestation from every recipient, no matter who that recipient is or what their purpose may be. After all, any non-HIPAA covered entity who obtains PHI can further use and disclose the PHI without regard to HIPAA's restrictions. Some recipients may be limited by other policies or laws, but many will not be limited in any way. Hospital lawyers who often and routinely over-interpret the privacy rule to demand protections beyond the established standard are likely to take no chances and may well seek attestations from all recipients.

If our guess is correct, this may actually be a good result because it highlights the need for privacy protections for PHI in the hands of non-HIPAA covered entity recipients. In fact, we suggest that the Department bow to the inevitable and require attestations in all cases. Further, we see no reason to stop at attestations that state that reproductive health information will not be used for a purpose inconsistent with the proposed standards in the rule. We would be happy if attestations also bound recipients so that they only used and disclosed PHI for the purposes for which they obtained the PHI. We can foresee some difficulties with a universal attestation policy. For example, we would allow exceptions for treatment disclosures to health care providers and perhaps under other circumstances.

What is important here is the idea of imposing restrictions on downstream recipients who are not today limited by HIPAA from using and redisclosing information as they please. We suggested above that data use agreements might serve the same purpose in place of or along side of attestations. We would support any reasonable method that has a chance of imposing restrictions on downstream recipients of PHI who are not themselves HIPAA covered entities.

---

[4] See, e.g., Pam Dixon and Robert Gellman, *Medical Identity Theft: The information crime that can kill you,* World Privacy Forum, May 3, 2006. https://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/ .

Nevertheless, we take a realistic view of the value of attestations. We are doubtful that the enforcement method for recipients who violate the terms of an attestation will be practical in many cases. It is more likely that the person requesting the information and who signs the attestation will not be the person who violates the terms. It may be a third person who obtained the information from the recipient who will violate the terms. Since that third person did not sign the attestation, no criminal or other penalty will attach. And since the person who signed the attestation did not violate its terms knowingly, enforcement against that person will also fail. Attestations signed on behalf of a department or agency may fail because the signer did not have authority to bind the department or agency.

Further, those who signed an attestation can pass information along to a third party who can then pass the information along through other hands. By the time the information lands in the hands of the police or prosecutors, the attestation given at the start will be forgotten and disassociated from the records that it applied to.

We do not have an immediate solution. However, if the Department specified that data subjects are third party beneficiaries of attestations (or data use agreements), that might provide an enforcement opportunity for anyone harmed by a prohibited use or disclosure of data. A civil enforcement action has a lower burden of proof than a criminal case.

Another reason that enforcement may fail is a lack of chain of custody for information that may end up in the hands of police or prosecutors. Consider a health oversight agency that receives information from multiple health care providers. A patient reported for possible violation of an abortion statute may have seen more than one provider (e.g., general practitioner, obstetrician, emergency room, urgent care facility, pharmacist, laboratory). It may be impossible to determine with sufficient certainty to support a criminal conviction that a particular data stream provided the data used for an improper purpose. Further, the same data covered by an attestation could also have originated from an informant, a health app, a merchant,[5] a search engine, or any of the other unregulated commercial or private sources of personal data. Commercial data brokers and list sellers may also provide information on pregnancy.[6]

VI. Administrative Requests by Law Enforcement Agencies

The current rule (45 CFR § 164.512(f)(1)(ii)(C)) allows for disclosures to law enforcement pursuant to administrative requests. The Department proposes to add language to clarify that a qualifying administrative request is one "for which a response is required by law." The discussion in the NPRM says that this is not a substantive change, only a clarification.

---

[5] See, e.g., Charles Duhigg, *How companies learn your secrets,* The New York Times Magazine, Feb. 16, 2012. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html . Also available at: https://charlesduhigg.com/new-york-times-magazine/ . This article describes how Target was able to analyze customer purchases and successfully predict a high school girl's pregnancy.

[6] See, e.g., MOMMIES TO BE Mailing List Data Card, Nextmark. https://lists.nextmark.com/market?page=order/online/datacard&id=466041. Retrieved 13 June 2023

We strongly support the clarification. We have not read the current rule as limited to administrative requests for which a response is *required by law* (e.g., administrative subpoena or summons; civil or authorized investigative demand, or similar process authorized under law). The current language is vague, and our reading of it has been that it permits oral requests by law enforcement officers. Frankly, when discussing this point with others in the HIPAA community, we never encountered anyone who read the existing provision as narrowly as the proposed clarification suggests. The Department reports that it is aware that some regulated entities may read the current language as allowing broader disclosures to law enforcement than the Department intended. A clarification is, indeed, in order. We are happy to be wrong in how we interpreted the language in question.

We cannot predict with any certainty the response to the clarification from the law enforcement community. Some who read the existing language as broadly as we have been reading it may raise objections.

We like the clarification, but we suggest it might create a better outcome to be more specific and refer to an administrative subpoena or summons, a civil or other expressly authorized demand, or a similar process expressly authorized by law. In the event that there are significant objections to the change, we want to share with the Department several of our long-time suggestions for narrowing the provision as we interpreted it in the past. That is, we consistently proposed that the rule should, at a minimum, 1) prohibit oral requests and 2) should require all informal administrative requests to be in writing. We also suggested that 3) qualifying administrative requests should require express supervisory approval.

The proposed clarification may make those suggestions unnecessary. We include them here in case they might be useful. We worry that lawmakers in states where terminations of pregnancy is restricted or illegal may devise new and procedurally simple disclosure requirements that would be "required by law" and might even not mandate a written request. As the Department knows, any disclosure required by law is lawful under HIPAA.

VII. HIPAA Waivers

During the COVID-19 emergency, the Department issued a variety of HIPAA waivers. Several years ago, WPF quietly published a report that analyzed the waivers in depth, and raised questions about the legality and content of the COVID waivers.[7] The issues identified in that report extend beyond COVID and address the waiver process generally. While we do not propose to repeat the arguments put forward in that report here, we note that even though the emergency has ended and the waivers are now withdrawn, many of the policy issues we raised in the report remain valid. We continue to urge the Department to take a comprehensive look at the use of HIPAA waivers, at the process for establishing new administrative policies about future waivers, and at the possible need for better legislation. Of course, we do not expect the Department to address those broader waiver

[7] World Privacy Forum, *COVID-19 and HIPAA: HHS's Troubled Approach to Waiving Privacy and Security Rules for the Pandemic* (2020), https://www.worldprivacyforum.org/2020/09/covid-19-and-hipaa/. We note that the National Committee on Vital and Health Statistics raised questions about HIPAA waivers in its December 15, 2022, letter to the Secretary regarding *Recommendations regarding Privacy, Confidentiality, and Security Considerations for Data Collection and Use During a Public Health Emergency*, https://ncvhs.hhs.gov/wp-content/uploads/2022/12/NCVHS-PHE-Letter-to-Secretary-FINAL-w-sig-508.pdf.

matters in this rulemaking. Some of the objectives in our earlier report relate to, but do not specifically address, the point we want to make here, however.

For COVID, the Office of Civil Rights (OCR) announced that it would exercise administrative discretion and effectively not enforce several specific HIPAA penalties. These actions were taken under what we called *administrative waivers* in the report. Whether or not you approve of our terminology, we use that same terminology here to discuss the possibility that the rule changes proposed in the NPRM could be the subject of further OCR exercises of administrative discretion. The Pandora's door to the use of administrative waivers of HIPAA rights has been opened, and we are concerned that now that the tool is available, its availability may become problematic in other areas.

Consider the possibility that another Administration might have a significantly different position on the protection of reproductive health information. Of course, a new Administration could change any rule that the Department adopts as a result of this rulemaking. There is little that can be done to avoid that possibility. Still, rulemakings take considerable time to complete.

Under the precedent established for COVID, OCR could, without going through a rulemaking, effectively eviscerate any protections to reproductive health information though a simple announcement of an administrative waiver. Based on the arguments we put forward in the 2020 report, we believe that there is a strong, but not conclusive, argument that this (and perhaps any) type of *administrative waiver* is illegal. It might, however, take several years before a court provided an authoritative decision on the legal argument.

We believe that the Department can and should take actions in the current rulemaking to prevent weakening of new limits on the use or disclosure of reproductive health information. HHS needs to limit OCR's ability to exercise general administrative discretion.[8] We see a number of possible ways to accomplish this.

One way is to amend the HIPAA privacy rule broadly to prevent the exercise of general administrative discretion by OCR on all parts of the HIPAA rule. The amendment would state that a formal rulemaking is required to change a practice mandated by the rule rather than through a broad statement of administrative discretion.

A second way is to amend the HIPAA privacy rule to prevent any blanket exercise of administrative discretion by OCR in the absence of a congressional declaration of emergency.

A third way is to add narrower language that would prevent the blanket exercise of administrative discretion with respect to any provisions relating to use or disclosure of reproductive health information added by the current rulemaking.

---

[8] We recognize that administrative discretion can be and is exercised on a case-by-case basis. We do not object to that. It is the broadly effective exercise of administrative discretion covering all actions of a particular type that is the focus of concern here.

Another idea would be to add one of these limits on blanket exercises of administrative discretion as a temporary measure. When the Department issues the final rule, the Secretary could concurrently task the National Committee on Vital and Health Statistics to study HIPAA waivers issues and report back. A temporary measure could expire a year (or at some other interval) after the filing of that report.

Changes to protect reproductive health information will have little long-term effect if a new Administration can on its first day in office issue a notice of administrative discretion saying that it will not enforce the protections added in this rulemaking. The Department should take action to prevent any simple method of overturning a new rule.[9]

Thank you again for the opportunity to comment on the proposed rulemaking. We appreciate the thoughtfulness of the NPRM. We stand ready to assist if you have any questions,

Respectfully submitted,

Pam Dixon,
Executive Director, World Privacy Forum

[9] We note that a statute allows the Secretary to waive application of some HIPAA provisions in the case of natural disasters. That authority would be unaffected by any of the rule changes we propose here.